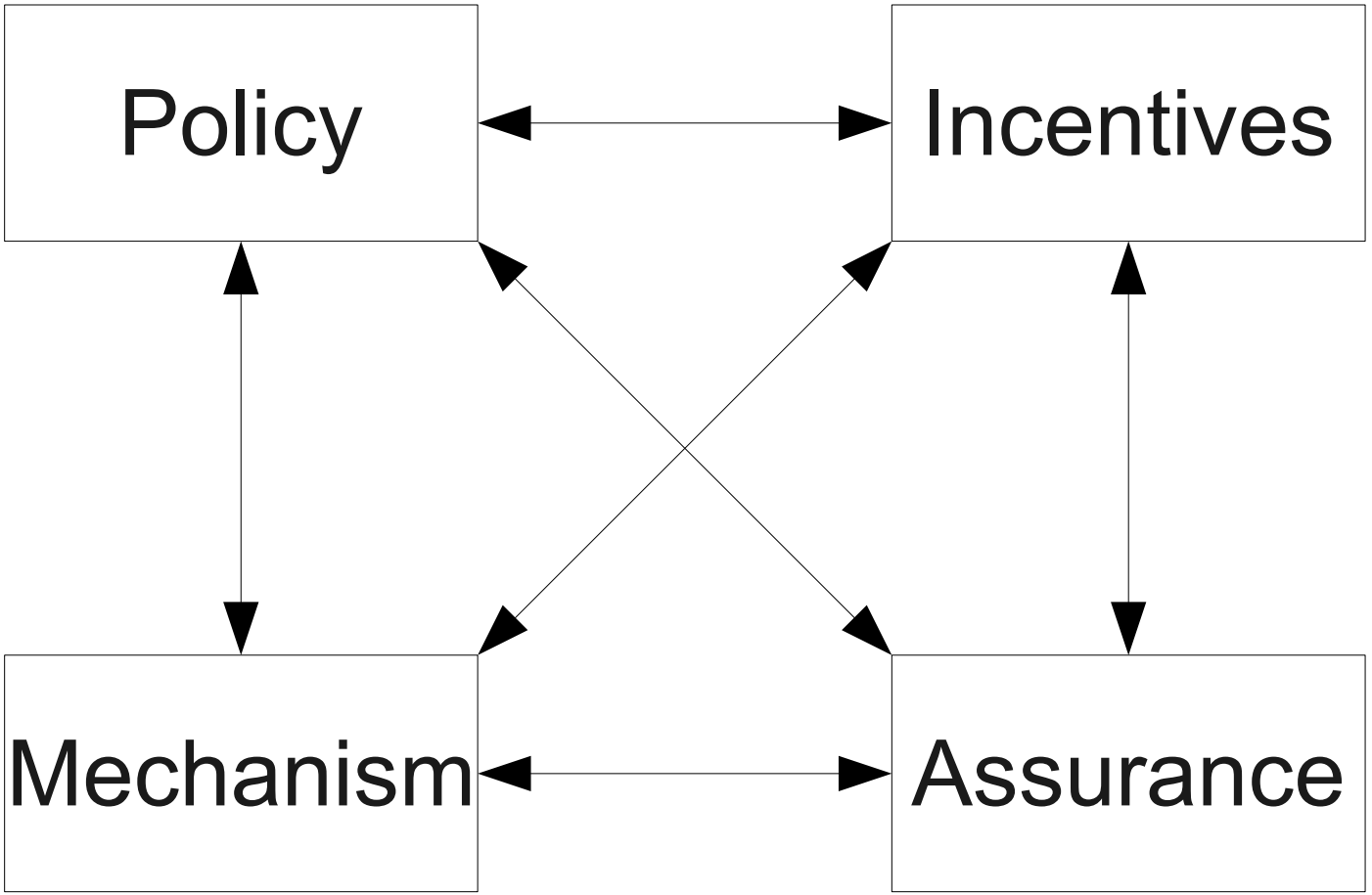
SECURITY ANALYSIS

In this Lecture

- How to analyse security of a system
- Notes on evaluating risk
- Classifying attackers

From „Security Engineering”



From „Security Engineering” (2)

- **Policy** – what you want to achieve
- **Mechanism** – technical tools you use to achieve the policy
- **Assurance** – amount of reliance you can place on any particular mechanism
- **Incentives** – motives of attackers and defenders

Example: Airport Security

- Policy – prohibit all weapons on board of planes
- Mechanism – screen passengers
- Assurance – poor, less than half of weapons are confiscated
  - Together with considerable amount of innocent items
  - Ground staff is not screened
  - Parked airplanes are not locked

Example: Airport Security (2)

- Problem is with incentives
- Visible controls are better than effective ones
  - Shows that we are doing something about the risk
- Incentive to exaggerate threat of terrorism
  - Politicians can scare people to vote for them
  - Journalists can sell more papers
  - Companies can sell more equipment
  - Government officials can strengthen their positions
  - Security researchers can get grants

Five Step Program

- Applicable for analyzing a security solution
- From „Beyond Fear” by Bruce Schneier

Step 1: Assets

- What assets are you trying to protect?
- What is the scope of the security measure?
  - Yourself?
  - Some number of people?
  - Whole country?

Step 2: Risks

- What are the risks to these assets?
- What is being defended?
- What the consequences are if the assets are successfully attacked?
- Who wants to attack it?
- Why?
- How they might attack it?

Step 3: Solution

- How well does the security solution mitigate those risks?
- How the solution interacts with the surroundings?
- How it works?
- How it fails?
- Requires knowing the security solution and its actual properties

Step 4: Other Risks

- What other risks does the security solution cause?

Step 5: Costs and Trade-Offs

- What costs and trade-offs does the security solution impose?
- How it interacts with other security measures, systems and your everyday life
- What else is needed to make it work?

An Example

- Should you avoid sending credit card numbers over the Internet?
  - Both E-mail and web count
- Step 1, assets: credit card number
- Step 2, risks: credit card theft
  - Especially, theft of your credit card
  - Hackers steal card numbers on the Internet
  - Note: in US, the maximum loss for customer is $50
    - Often waived in the event of fraud
  - After compromize, you have to get new credit card, update card number in various sites

An Example (2)

- Step 3, solution: does not have effect on credit card theft
  - Attackers steal credit card data from merchant databases
    - Much easier than attack individual users
  - Credit card number is in database regardless of the medium (Internet, mail, telephone)

An Example (3)

- Step 4, other risks: none?
- Step 5, costs and trade-offs:
  - Convenience
  - Cannot take advantage of good prices
- Conclusion: countermeasure does not mitigate risk, but introduces additional costs. Probably not worth it.

Evaluating Risks

Evaluating Risks

- For companies it's easier: all risks can be converted to money
  - Loss of life = cost of lawsuit and damages
  - Bad publicity = loss of sales, cost of rebuilding good image
  - Bankrupcy = all shareholders lose their shares
  - However, ome risks can also threaten personal freedom of executives

Evaluating Risks (2)

- Governments must balance human life, human rights etc. with money
  - How much money to spend on military?
  - Should we send infantry or air force?
  - How much to spend on police?
  - Should we reduce people's rights to increase security?
- Civil engineers always know the cost of human life?

Evaluating Risks (3)

- Some risks are not acceptable to some people
  - Meaning: we cannot build a system where this risk exists, no matter how improbable
- Examples:
  - Nuclear power plant
  - Genetically engineered crops

Perception of Risks

- People exaggerate spectacular but rare risks, but downplay common risks
  - Earthquakes vs. slipping on bathroom floor
  - Terrorism vs. street crime
- People incorrectly estimate risks for situations not exactly like their normal life

Perception of Risks (2)

- Personified risks are perceived as greater than anonymous risks
  - „The death of one man is a tragedy, the death of millions is a statistic."
  - Automobile deaths vs. 9 people trapped in a mine
- People underestimate risks they take willingly and underestimate risks in situations they cannot control
  - Driving in car vs. flying on airplane

Perception of Risks (3)

- People overestimate risks that are talked about
- However, this does not mean that the risk is very common
  - News are news because they happen rarely

For Example…

- AIDS kills 3 million every year – compare with SARS, swine flu etc.
- Lunatic is fired, goes back to office and kills boss and two coworkers – national news
- Lunatic goes home and shoots ex-wife and two kids – local news
- In America, 40 000 automobile deaths every year
  - Equal to fully loaded Boeing 727 crashing every day and a half
- More people are killed by pigs than sharks

Who Are the Attackers?

Professional Criminals

- Does crime because it pays money
- „Because that's where the money is." -- Willie Sutton on why he robs banks
- Main goal is money. Stealing information can lead to money
- Calculated risk, depending on chance of getting caught and severity of punishment

Professional Criminals (2)

- Have varying amount of resources and access to the system
- **Insiders** have good access to system
  - Many (most?) successful crimes involve insiders
  - Can work for themselves or for outsider group
  - Can be tricked by outsiders

Opportunists

- One-off criminals
- Tempted by good opportunity
- Often insiders
- Usually risk averse

Emotional Attackers

- For example:
  - Revenge
  - Crimes of passion
  - Vandalism (for fun)
  - Bar fight
- Often *statement attacks*
- Can accept greater risks than professional criminals
  - Suicide by cop
  - Running amok

Emotional Attackers (2)

- The attack is often DOS type – no gain for the attackers
- Very hard to defend against. Cannot say „this attack is not worth it”

Friends and Relations

- Special class of insiders
- Significant amount of credit card fraud is performed by card owner's relatives
- Mostly opportunists
  - Look at private data

Industrial Competitors

- Mostly industrial espionage
- Often well-funded
- Example: GM executive went over to VW and took with him many confidential documents
  - VW paid $100M in damages and agreed to buy $1B of parts
- Constant spying accusations between Boeing and Airbus

Industrial Competitors (2)

- Often investigative journalism plays the same role
- Tabloids were willing to pay $500K for compromising photos of princess Diana
- Reporters often take many risks
  - Sometimes are willing to go to jail, if they believe they fight for just cause

Governments

- Especially police departments
  - Against criminals, police are attackers
  - In oppressive governments, police works for corrupt government
  - Rogue policemen
    - J. Edgar Hoover used FBI as private enforcement tool

Governments (2)

- Generally quite risk averse
- Some attacks are less risky for police
  - With search warrant, breaking and entering is not a crime
- Intelligence organizations
  - Extremely well funded
  - Very risk averse and publicity averse
  - Stolen information is more powerful if it is secret
    - The Enigma example
  - Public scandals expose techniques, capabilities and sources

Terrorists

- Use displays of violence for political goals
- Primary aim is to make a statement
  - News of the attacks are more important than the attacks themselves
- Extremely hard to defend against
  - Effective tactic would be to deny access to media
- When analysing motivations, think „who has more to lose”

Notes on Attacks

What is the target of attack?

- You specifically?
- Specific kind of targets?
- Any target?
- Many everyday security systems are designed to make attacker go somewhere else
  - Alarms, cameras, car alarms
- If you have something good, expect targeted attacks

Different Agendas

- Example: you want to spend your money
- You are not interested in detecting counterfeits
- Counterfeits is government's problem – affects the monetary system
  - In fact, governments spend more money on fighting counterfeiting than are the losses caused by counterfeinting

Different Agendas (2)

- Example: kidnapping
- It is in the interest of kidnappee to pay money
- Government/police tries to avoid paying money
  - Paying money encourages future kidnappers
- Survival of individual vs. survival of species

Different Agendas (3)

- People are often represented by proxies
  - Lawyers, inspectors, auditors
- Proxies can have their own agendas

Class Break

- Somebody figures out how to break one system
- This knowledge is applicable to all installations of the system
- Examples:
  - Locks, alarms
  - Software
  - Phone hacking
  - Using EEK coins as DM
  - Cable TV fraud

Automation

- Can make some attacks effective
- Example: attack succeeds once per 100 000 tries
- Example: ttack yields 0,1 cents

Recap: Cornerstones of Security

- Prevention
- Detection
- Response

Prevention

- Prevention is usually not absolute
- Typically prevention measures buy you time
- Example: safes
  - TL 30 – safe can resist professional safecracker with tools for 30 minutes
  - TL-TR 60 – professional safecracker with tools and oxyacetylene toch for 60 minutes
  - Sustained attack: only actual time spent on cracking is counted (no rest breaks)
  - Attacker has drawing for the safe

Prevention (2)

- Safe is meaningless if criminal can work on it all night
- Because no prevention measure is absolute, you need detection and response
- Safe example: you must have alarms and the police must arrive within 30 (60) minutes

Detection

- Example: credit card fraud
- Prevention is impossible
- Focus on detection (behaviour profiling) and response (refund the money for customer)

Detection (2)

- Some detection measures can double as prevention measures
  - Visible guards, cameras
  - „This building is protected by alarm”
- Message: „Go rob somebody else”
- Not so useful for targeted attacks

Detection (3)

- Random detection: only check some objects/persons/etc.
- Example: bus tickets, speed traps
- Works if punishment exceeds the crime
  - Otherwise it is rational to pay the occasional fine

Active and Passive Failure

- **Passive failure** – security measure fails to stop the threat
- **Active failure** – security measure takes action when it shouldn't
- In general, active failures are less tolerated
- Problem when attacks are rare and false alarms are frequent
  - Example: car alarms

Detection (4)

- **Audit** – reviewing data to catch attacks and errors
- Used everywhere
- Most surveillance cameras are used for audit rather than real-time detection
- **Prediction** – trying to detect attack before it happens
- Requires accurate information about the situation

Response

- **Reaction** – do something about the attackers
- Usually: invoke additional countermeasures
- Example: automatically lock all doors when alarm is triggered
- **Mitigation** – do something about the assets
- Examples:
  - Automatic fire extinguisher
  - Suspend credit card when fraud is detected

Response (2)

- **Recovery** – repair the damage after attack
- Restoring from backup
- After recovering the system, you can be open for another attack
- **Forensics** – collect and analyse evidence
- Goal: catching attackers or preventing further attacks
- Usually in conflict with recovery

Response (3)

- **Counterattack** – attack the attackers
- Can be retaliation or attempt to disable the attacker
  - Legal prosecution can be considered the latter
- In civilian matters, counterattack is usually illegal

Thank You

- Questions?